JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Review of Secure Key Algorithms and Protocols for Sharing Information in VANET Systems

[1]Chetan Singh, [2]Shushila Sonare
[1]Research Scholar, [2]Assistant Professor
Department of Computer Science & Engineering,
Lakshmi Narain College of Technology, Bhopal, India

Abstract : Vehicular Ad hoc Networks (VANET) is a subgroup of (Mobile Ad Hoc Networks) MANET which is using for improves traffic safety system. Since the movements of Vehicles are restricted by roads, traffic regulations we can deploy fixed infrastructure at critical locations. We focus our study on the different kind of attacks based on security algorithm and protocol and routing. In this paper we review secure key algorithms and protocols for sharing information in VANET Systems. After surveying we found that attacks in multilayer are very harmful for security system as well as authentication and privacy are big challenges.

IndexTerms **- VANET, MANET, DOS, Attack, Protocol, Routing.**

I. INTRODUCTION

In the VANET systems, the leakage of some sensitive data or communication information will cause heavy losses for life and property. Then, a higher security level is required in the VANET systems. Meanwhile, fast computation powers are needed by devices with limited computing resources. Thus, a secure and lightweight privacy-preserving protocol for VANETs is urgent. Vehicular Ad-Hoc NETworks (VANETs) have recently turned out as an auspicious way to raising road safety and efficiency while providing the opportunity to enhance driver's performance and attention. This can be achieved via a diversity of applications that implicate communication between vehicles, like alerting other vehicles about a parking brake or an eventual emergency case. Nevertheless, the lack of an efficient secure routing protocol may cause the interesting properties of VANETs to ultimately outcome in greater dangers of maltreats. Indeed, the routing process is subject to various threats since it is the basic mechanism that assures both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.

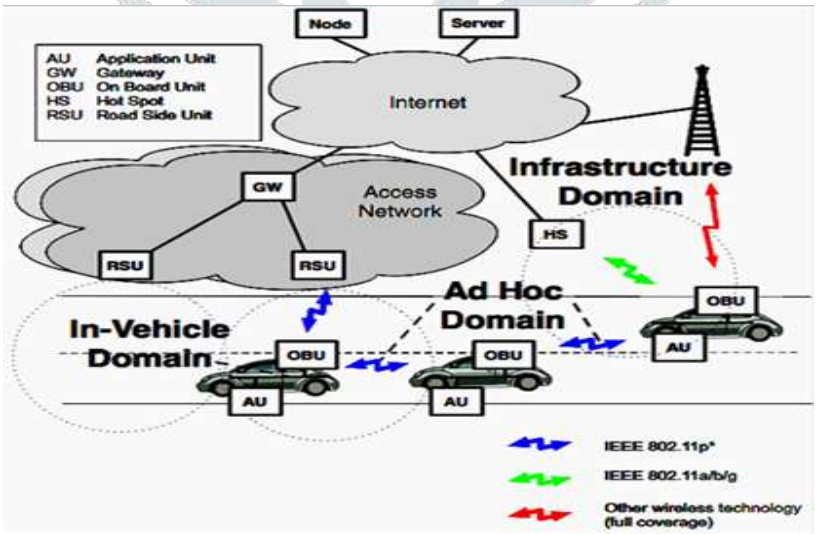

Figure 1: VANET System

These phenomena amplify when the number of vehicles increases due to the rise in the rate of exchanged packets. Thus, securing the routing operation in VANET has become of a major concern. As the crucial component of intelligent transportation system, vehicular ad hoc networks (VANETs) are capable of providing a variety of safety-related functionalities and commercial-oriented applications, which significantly improves the driving experience. Due to the foreseen impact of VANETs, extensive studies in both academia and industry fields has been made, which emphasizes on effective VANETs implementations.

In practical VANETs scenarios with open wireless communication characteristics, enhanced security strategies should be deployed in order to guarantee transmission safety. Moreover, individual vehicle needs to perform pre-defined authentication process toward all the acquired messages, some of which may be generated by abnormal devices or malicious attackers. In this case, with

large amounts of anomaly messages to be authenticated during a relatively short time period, the denial of service (DoS) attack is possible. Note that the vehicle has limited computation capability and restrained storage.

In vehicular ad hoc networks (VANETs), vehicles communicate with each other and with roadside units (RSUs) in order to enhance road safety, improve traffic management and provide infotainment services. Along with the growth of VANETs, some challenges are emerging. Although there are many research work on VANETs, cheating attacks are still not well resolved such as selective message relaying attack, faked information reporting attack and resource-consuming attack launched by selfish or malicious participants. Vehicular Ad hoc Network (VANETs) allows the vehicles on the roads to form a self-organized network and is blooming up in a exotic way to support intelligent transportation services. In VANETs, the vehicles are the nodes and hence move at very high speed leading to frequent changes in topology resulting in loss of data that causes failure in data reliability.

II. BACKGROUND

C. Chen et al.,[1] presents a digital signatures mechanism, key agreement and authentication scheme to satisfy the security requirements for a VANET. Burrows-Abadi-Needham logic (BAN logic) is applied to prove that the proposed scheme achieves secure authentication. The proposed protocol ensures the privacy of the communication between fleets and provides a mechanism for immediate emergency reporting. The experiment results show that the proposed scheme is feasible and meets security requirements.

S. Kanchan et al.,[2] We propose a secure authentication algorithm to efficiently re-encrypt the messages using signcryption. For faster computation and routing, the authors have used shareable clouds in VANET groups. Security of the protocol is proved using Burrows-Abadi-Needham logic and validated by simulation tool automated validation of internet security protocols and applications.

Z. Wei et al.,[3] propose an identity-based signature that achieves unforgeability against chosen-message attack without random oracle. In order to reduce the computational cost, we design two secure and efficient outsourcing algorithms for the exponential operations, where a homomorphic mapping based on matrices conjugate operation is used to achieve the security of both exponent and base numbers. Furthermore, we construct a privacy-preserving protocol for VANETs by using outsourcing computing and the proposed IBS, where a proxy re-signature scheme is presented for authentications.

M. Ma et al.,[4] design a new authenticated key agreement protocol without bilinear pairing. This protocol achieves mutual authentication, generates a securely agreed session key for secret communication, and supports privacy protection. We also give a strict formal security proof and demonstrate how the proposed protocol meets the security requirements in the fog-based VANETs. We then evaluate the efficiency of the proposed protocol, and it shows the practicality of the protocol.

A. Slama et al.,[5] propose a new Trust Cryptographic Secure Routing protocol for VANETs, baptized TCSR protocol. The key idea is to reuse the AIMD (Additive Increase Multicative Decrease) algorithm. To avoid scalability problems and high level of processing, this scheme fixes a threshold trust level allowing each node to communicate with the others in the network associated to plausibility checks in order to calculate the node score. Since the node with the most appropriate score is selected, asymmetric cryptography is used to secure the transferred packet carrying the routing information. The performance analysis shows that TCSR protocol is efficient in terms of verification delay and average throughput.

H. Tan, et al.,[6] presents the above issues by developing a secure and efficient authentication scheme with unsupervised anomaly detection. In our design, certificate less authentication technique is deployed for conditional privacy preserving, along with the Chinese remainder theorem for efficient group key distribution and dynamic updating. Subsequently, the corresponding unsupervised anomaly detection method is illustrated, which applies dynamic time warping for distance measurement.

D. K. Sandou et al.,[7] provides high security, less network delay and better packet delivery ratio compared to the existing protocol. The test bed scenario is implemented using NS2 tool for simulation analysis and the same has been analyzed to obtain the performance metrics.

H. Tan et al.,[8] proposed scheme is resistant to replay attack and masquerade attack. However, we find that the proposed scheme given by Vijayakumar et al. is still vulnerable to replay attack, which could be conducted by reusing previously acquired messages. Moreover, this scheme cannot resist masquerade attack toward the system. For the above consideration, in this paper, modifications toward the existing protocol are presented, so as to provide adequate security assurance toward the mentioned attacks.

E. R. Agustina et al.,[9] Numbers of secure VANET protocols have been proposed to solve this issue, but privacy has received less attention. In this paper, we proposed a secure VANET protocol which guarantees privacy and authentication via hierarchical pseudonyms with blind signature. Furthermore, we analyzed our protocol using Scyther Tool for protocol verification. The result shows that our protocol achieved the security claims.

K. Lim, et al.,[10] propose an efficient key management protocol for group signature based authentication, where a group is extended to a domain with multiple road side units. Our scheme not only provides a secure way to deliver group keys to vehicular nodes, but also ensures security features. The experiment results show that our key distribution scheme is a scalable, efficient and secure solution to vehicular networking.

S. Chaba et al.,[11] proposes the design of the framework for vehicular ad hoc networks (VANET) for delivery of the authentication keys with minimum delay amongst vehicles having high mobility using fog and cloud computing. We propose to introduce fog computing to extend cloud computing by introducing an intermediate fog layer between mobile devices and cloud thus producing a number of advantages.

L. Wei et al.,[12] To deal with this kind of attacks, we present two novel lightweight security mechanisms by equipped each vehicle's On-Board Unit (OBU) with a small elegant module called TrInc, which is a trusted hardware and composed of only a non-decreasing counter and a key. We observe that TrInc-based method not only can effectively resist against cheating attacks in safety-oriented, convenience-oriented, and commercial-oriented VANET applications, but also significantly defend various aspects of security and privacy in VANETs.

III. CHALLENGES AND ATTACKS

The main challenge of VANET system is security issue and performance of various protocols.

- Security and mutual reliability are the crucial requirements of an ad hoc network as nodes are dependent upon each other for routing and forwarding their messages. Vehicular ad hoc networks (VANETs) are no exception and are always at the risk of impersonation attack. An authentication protocol protects the identity of network entities from being impersonated. Occasionally, they require re-encryption technique which enables any other node to communicate on behalf of an unavailable node. The technology is used to provide backup in emergencies.

- The main objective of deploying Vehicular Ad-hoc Network (VANET) is to reduce the accidents level by providing traffic information to the driver to drive safely. Since VANET supports emergency real-time applications and deals with human life critical information, the security of VANET becomes one of the most critical issues.

Table 1: Comparison of different security approaches

Parameter	**Privacy Preserving**	**ID Crypto**	**Token**	**Frame-Work**
Properties	Infrastructure Based	Signature Encoding	Topology	Used at Data link layer
Complexity	Less	High	Very less	High
Through put	High	Average	Very less	High
Cost	High	Very less	Less	Less
Time	Medium	Less	Very High	Very less
Range	10 km	1-2 km	10 km	1-2 km

ATTACKS

• Jamming

The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

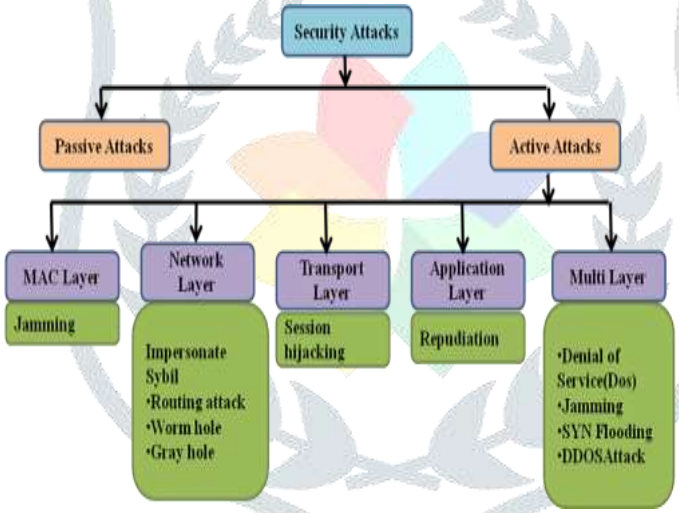

Figure 2: Classification of attacks based on Layers

• Node Impersonation Attack

Each vehicle has a unique identifier in VANET and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles [4, 9, and 10]. Fig explains this scenario in which vehicle A involves in the accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it.

Figure 3: Node Impersonation Attack

• Sybil Attack

Sybil attack [10] so belongs to the first class. In Sybil attack, the attacker sends multiple messages to other vehicles and each message contains different fabricated source identity (ID). It provides illusion to other vehicle by sending some wrong messages like traffic jam message [3, 4]. Fig 5 explains Sybil attack in which the attacker creates multiple vehicles on the road with same identity. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker.

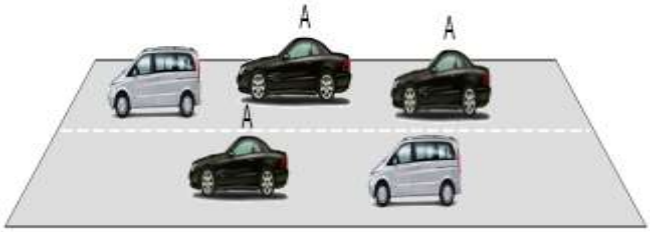

Figure 4: Sybil Attack

IV. ROUTING ATTACK

Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:

a) Black Hole attack:

In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

b) Wormhole attack:

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

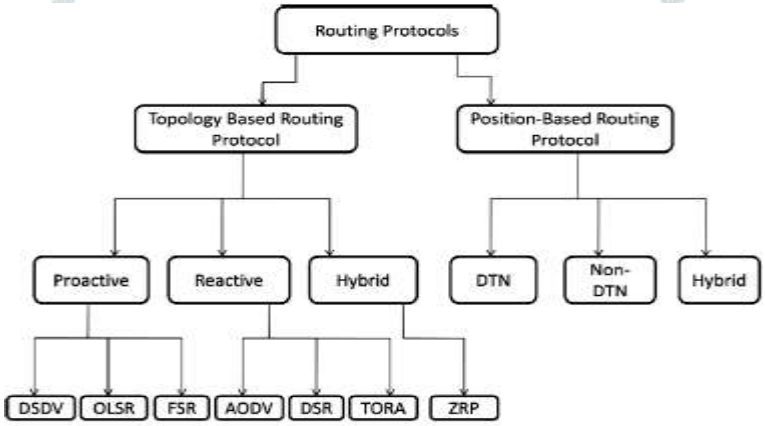

Figure 5: Different Routing Protocol

c) Gray Hole attack:

This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two types:

i) A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.

ii) The malicious node can drop the packet on the basis of probabilistic distribution.

• Session hijacking

Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

Repudiation: The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

• Denial of Service

DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways.

a) Jamming: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

b) SYN Flooding: In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

c) Distributed DoS Attack: This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

V. CONCLUSION

This paper includes various attacks in VANET have been classified depending on the different layers. It has been observed that the classification helps to deal with different types of attack in VANET. We have been discussed security challenge and security requirements. We have found after survey that attacks in multilayer are very harmful for security system as well as authentication and Privacy are big challenges. In future we analyze vehicular network using multi encryption and suitable routing and protocols prevention method.

REFERENCES

1. C. Chen, Y. Chen, C. Lee, Y. Deng and C. Chen, "An Efficient and Secure Key Agreement Protocol for Sharing Emergency Events in VANET Systems," in IEEE Access, vol. 7, pp. 148472-148484, 2019, doi: 10.1109/ACCESS.2019.2946969.
2. S. Kanchan, G. Singh and N. S. Chaudhari, "SAPSC: SignRecrypting authentication protocol using shareable clouds in VANET groups," in IET Intelligent Transport Systems, vol. 13, no. 9, pp. 1447-1460, 9 2019, doi: 10.1049/iet-its.2018.5474.
3. Z. Wei, J. Li, X. Wang and C. Gao, "A Lightweight Privacy-Preserving Protocol for VANETs Based on Secure Outsourcing Computing," in IEEE Access, vol. 7, pp. 62785-62793, 2019, doi: 10.1109/ACCESS.2019.2915794.
4. M. Ma, D. He, H. Wang, N. Kumar and K. R. Choo, "An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8065-8075, Oct. 2019, doi: 10.1109/JIOT.2019.2902840.
5. Slama, I. Lengliz and A. Belghith, "TCSR: an AIMD Trust-based Protocol for Secure Routing in VANET," 2018 International Conference on Smart Communications and Networking (SmartNets), Yasmine Hammamet, Tunisia, 2018, pp. 1-8, doi: 10.1109/SMARTNETS.2018.8707389.
6. H. Tan, Z. Gui and I. Chung, "A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs," in IEEE Access, vol. 6, pp. 74260-74276, 2018, doi: 10.1109/ACCESS.2018.2883426.
7. D. K. Sandou, N. Jothy and K. Jayanthi, "Secured Routing in VANETs Using Lightweight Authentication and Key Agreement Protocol," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2018, pp. 1-5, doi: 10.1109/WiSPNET.2018.8538678.
8. H. Tan, D. Choi, P. Kim, S. Pan and I. Chung, "Comments on "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks"," in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2149-2151, July 2018, doi: 10.1109/TITS.2017.2746880.
9. E. R. Agustina and A. R. Hakim, "Secure VANET protocol using hierarchical pseudonyms with blind signature," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-4, doi: 10.1109/TSSA.2017.8272919.
10. K. Lim, K. M. Tuladhar, X. Wang and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 478-483, doi: 10.1109/UEMCON.2017.8249091.
11. S. Chaba, R. Kumar, R. Pant and M. Dave, "Secure and efficient key delivery in VANET using cloud and fog computing," 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, 2017, pp. 27-31, doi: 10.1109/COMPTELIX.2017.8003932.
12. L. Wei and C. Zhang, "TrInc-Based Secure and Privacy-Preserving Protocols for Vehicular Ad Hoc Networks," 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, 2016, pp. 1-5, doi: 10.1109/VTCSpring.2016.7504512.
13. P. Vijayakumar, M. Azees, A. Kannan and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 1015-1028, April 2016, doi: 10.1109/TITS.2015.2492981.
14. M. Nema, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375676.